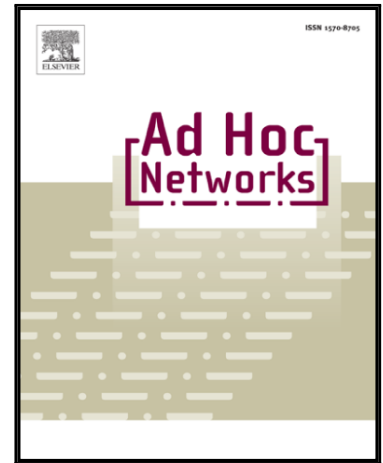


## Accepted Manuscript

ICMDS: Secure Inter-Cluster Multiple-Key Distribution Scheme for Wireless Sensor Networks

Amjad Mehmood , Muhammad Muneer Umar , Houbing Song

PII: S1570-8705(16)30282-7  
DOI: [10.1016/j.adhoc.2016.10.007](https://doi.org/10.1016/j.adhoc.2016.10.007)  
Reference: ADHOC 1475



To appear in: *Ad Hoc Networks*

Received date: 3 April 2016  
Revised date: 19 September 2016  
Accepted date: 6 October 2016

Please cite this article as: Amjad Mehmood , Muhammad Muneer Umar , Houbing Song , ICMDS: Secure Inter-Cluster Multiple-Key Distribution Scheme for Wireless Sensor Networks, *Ad Hoc Networks* (2016), doi: [10.1016/j.adhoc.2016.10.007](https://doi.org/10.1016/j.adhoc.2016.10.007)

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.

# ICMDS: Secure Inter-Cluster Multiple-Key Distribution Scheme for Wireless Sensor Networks

Amjad Mehmood<sup>1</sup>, Muhammad Muneer Umar<sup>2</sup>, Houbing Song<sup>3</sup>

<sup>1</sup>Guangdong Provincial Key Laboratory on Petrochemical Equipment Fault Diagnosis

Guangdong University of Petrochemical Technology, Maoming, Guangdong 525000 China

<sup>2</sup>Department of Management & Information Technology, Jubail Industrial College, Royal Commission for Jubail & Yanbu

Jubail Industrial City, 31961 Kingdom of Saudi Arabia

<sup>1,2</sup>Institute of Information Technology, Kohat University of Science & Technology, Kohat, 26000 Pakistan

<sup>3</sup>Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV 25136 USA

Email: <sup>1</sup>[amjadiitkust@gmail.com](mailto:amjadiitkust@gmail.com), <sup>2</sup>[muneerumar@hotmail.com](mailto:muneerumar@hotmail.com), <sup>3</sup>[h.song@ieee.org](mailto:h.song@ieee.org)

Corresponding Author: Houbing Song

## Abstract

In wireless sensor networks (WSNs), a large number of nodes are densely deployed in an open environment to gather some useful required information. These nodes are small in size, operating on limited processing capabilities with scarce working memory and battery life and not very powerful radio transceivers. They can only communicate with each other through wireless media. Radio waves are insecure in nature; therefore, by using such waves for communication there are always opportunities for different attacks on the network. Most wireless techniques are founded on the cluster-based sensor network. Forwarding *cluster head's* (CHs) data in a secure manner is very important because CHs collect data from the cluster members and send it to the sink node or base station. For securing CH's data, we propose a mechanism termed ICMDS (Inter-Cluster Multiple Key Distribution Scheme for Wireless Sensor Networks), which enables the securing of the entire network. In ICMDS, we use two phases of security implementations for the sensor node's authenticity while communicating with the CH. A recovery phenomena is also stated at the time when a CH ceases to function due to its high energy consumption.

**Keywords:** ICMDS, CH, Clustering, Security, Digital Signature, Cryptography, Authentication, Key Based, Distributed key, Pre-distributed, Secure Network, Public Key, Private Key.

## 1. Introduction

Wireless sensor networks (WSNs) have applications in all walks of life. Their popularity is increasing everyday due to their direct effect on human life. WSNs assist in many fields such as environmental analysis, medical diagnosis, military applications, underground analysis, and exploring planets [1-6].

A WSN is categorized as a self-organized ad hoc network [7]. In such network, a number of sensor nodes are widely spread around an area [7]. Nodes in these networks are tiny, relatively inexpensive and limited-power battery-operated devices [8]. For utilizing such nodes, many methods have been proposed regarding the energy efficiency and elongation of the network [9-14]. Sensor nodes group together to form a cluster. In each cluster a single node is selected as a Cluster Head (CH) [15-19], while the remaining nodes become member nodes. Member nodes sense environmental data and transmit it to the CH. The CH's responsibility is to aggregate that data and transmit it to the base station or sink node [20]. There are a number of protocols which have been proposed for the selection of an optimal CH [12,14,21].

Download English Version:

<https://daneshyari.com/en/article/4953639>

Download Persian Version:

<https://daneshyari.com/article/4953639>

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