International Journal of Innovative Computing, Information and Control
Volume **5**, Number **12(A)**, December **2009**

ICIC International ©2009 ISSN 1349-4198
pp. **4693–4702**

A GA-BASED KEY-MANAGEMENT SCHEME IN HIERARCHICAL WIRELESS SENSOR NETWORKS

Chien-Lung Wang[1], Tzung-Pei Hong[2,3], Gwoboa Horng[1]
and Wen-Hung Wang[4]

[1]Department of Computer Science
National Chung-Hsing University
Taichung 402, Taiwan
{ phd9004; gbhorng }@cs.nchu.edu.tw

[2]Department of Computer Science and Information Engineering
National University of Kaohsiung
Kaohsiung 811, Taiwan

[3]Department of Computer Science and Engineering
National Sun Yat-sen University
Kaohsiung 804, Taiwan
tphong@nuk.edu.tw

[4]Taichung Commercial Bank
Taichung 400, Taiwan
wh.wang123@gmail.com

Received July 2008; revised December 2008

Abstract. *In this paper, we propose a novel key management scheme based on genetic algorithms to fulfill the requirement of power control, memory usage and computation security in a hierarchical wireless sensor network. We divide the scheme into three parts: the sink node, the header node and the sensor node. The sink node first uses genetic algorithms to generate appropriate key-generating functions, and then deliver them to header and sensor nodes. Each possible key-generating function is encoded as a chromosome, which is feasible if it satisfies the specified power-consumption constraint. Its fitness is set as the entropy measure for evaluating key distribution. The final key-generating functions are then gathered for rekeying. The header and the sensor nodes can then assemble common keys from the key-generating functions for communication. The proposed scheme is simple, efficient and secures if the sensor nodes cannot be compromised within a threshold time bound. Experiments are also made to show its performance.*

Keywords: Power consumption, Key-generating function, Genetic algorithm, Security, Hierarchical sensor network

1. **Introduction.** Wireless sensor networks (WSN), a kind of ad hoc networks [7,9,10,17, 20,22], are widely used in a variety of applications [21]. In a WSN, sensor nodes are deployed in different locations to be responsible for perceiving local information and reporting to sink nodes. When sensor networks are deployed in a malicious and hostile environment, security would be extremely important. For example, a malicious adversary can easily eavesdrop or interpolate the communicated information, and can thus intentionally provide the misleading information to other nodes or impersonate one of the network nodes.

A sensor node is usually limited by its computing capability, memory size, communication protocol, and battery energy. These constraints make the encryption algorithms using public keys infeasible to sensor nodes since their computing power can not handle