International Journal of Innovative Computing, Information and Control
Volume **6**, Number **2**, February **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 809–816

A KEY MANAGEMENT SCHEME FOR SENSOR NETWORKS USING BILINEAR PAIRINGS AND GAP DIFFIE-HELLMAN GROUP

Iuon-Chang Lin[1], Pen-Yi Chang[2] and Chin-Chen Chang[3]

[1]Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan
iclin@nchu.edu.tw

[2]Department of Computer Science and Information Engineering
National Chung Cheng University
Chaiyi, Taiwan

[3]Department of Information Engineering and Computer Science
Feng Chia University
Taichung, Taiwan

Received July 2008; revised December 2008

Abstract. *To make wireless sensor network more suitable in practical use, researchers have to develop an efficient method to ensure secure data transmission through sensor nodes. Since sensor nodes do not have good computational ability, it is hard to be applied in complex computations, such as exponential computation to design a key management scheme. Therefore, the existing key management schemes in sensor networks usually employ the method of random key pre-distribution to achieve the security of communications and reduce the overheads of computations and storage. However, random key pre-distribution method has a drawback that any pair of sensor nodes cannot guarantee to hold the same shared key to construct a secure channel in between. In this paper, we are going to propose a novel key agreement scheme which can ensure that any pair of node can securely negotiate one session key. Furthermore, the required computational overheads are acceptable because the scheme is based on Bilinear Pairing and Gap Diffie-Hellman Group. As a result, our scheme is more suitable for being applied in wireless sensor networks.*

Keywords: Key agreement, Bilinear pairing, Gap Diffie-Hellman group, Sensor networks

1. **Introduction.** In recent years, wireless sensor network is booming because of the mature of wireless network and its variety in applications [10, 16, 22, 29]. So far, wireless sensor network can be used in military sensing and tracking, environment monitoring, patient monitoring, pollution monitoring, etc. In a sensor network, sensors are employed in the extreme environment, like the edge of volcano or war field, to monitor the activity of volcano or to detect the toxic gas. However, if a malicious user can counterfeit the information between nodes, it would be a loophole. Thus, secure communication is a very important requirement in wireless sensor network [1]. Message encryption techniques, such as DES and AES, are widely used to achieve the confidentiality of transmitted data. And, how to share the same session key between the sensor nodes becomes the major problem and some key distribution schemes [4, 24] are necessary.

In order to develop a key agreement scheme suitable for sensor network, we have to consider the following properties.

1. Low bandwidth and low computation ability.